Sarkisian, Richard Gabriel

WEIL NUMBERS AND FORMS FOR VARIETIES OVER FINITE FIELDS

City University of New York PH.D. 1984

WEIL NUMBERS AND FORMS FOR VARIETIES OVER FINITE FIELDS

by

RICHARD SARKISIAN

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

1984

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

August 15, 1984
Date

Raymond T. Hoobler
Chairman, Examining Committee

August 15, 1984
Date

Martin Marsboury
Executive Officer

Raymond T. Hoobler
Alfonse Thomas Vasquez
Harvey Cohn
Supervisory Committee

The City University of New York

ACKNOWLEDGMENTS

This thesis could not have been written without the help and encouragement of my thesis advisor, Ray Hoobler. Discussions with Al Vasquez and others at the CUNY Graduate Center have been helpful. More personally, I acknowledge the patience and support of my parents over many years. It is to them that I dedicate this thesis.

TABLE OF CONTENTS

Chapter 0.

Background and Motivation

Let X be a smooth algebraic variety defined over the finite field $\mathbb{F}_q$ with $q=p^a$ elements, where p is a prime integer. The zeta function $Z(X,t)$ associated to X is defined by

$$Z(X,t) \equiv \exp\left(\sum_{s=1}^{\infty} \frac{N_s}{s} t^s\right) .$$

This is a formal power series, where N_s is the number of F_{q^s} - rational points of X. This definition has a long history (see Katz [9]). An important type of algebraic varieties are abelian varieties.

Definition. (Lang [10], Mumford [14], Weil [26]). An abelian variety is a complete projective variety with algebraic group law.

To an abelian variety X we can associate a $\mathbb{Q}_\ell$-vector space, where $\mathbb{Q}_\ell$ is the field of ℓ-adic rationals (without further mention we assume that X is defined over $\mathbb{F}_q$ and that ℓ is a prime number, $\ell \neq p$). For each positive integer $n \geq 1$, let $X_{\ell^n} = \{x \in X \mid \ell^n x = 0\}$. There is a map $\ell: X_{\ell^{n+1}} \to X_{\ell^n}$ which sends $x \to \ell x$. Form the sequence $\ldots X_{\ell^{n+1}} \xrightarrow{\ell} X_{\ell^n} \longrightarrow X_{\ell^{n-1}} \longrightarrow \ldots \xrightarrow{\ell} X_\ell$ and take the inverse limit of this diagram, $T_\ell(X) \equiv \varprojlim_n X_{\ell^n}$. Then $T_\ell X \cong \mathbb{Z}_\ell^{2g}$ where $g = \dim X$, since $X_{\ell^n} \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$. Let $V_\ell X = T_\ell X \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell^{2g}$. V_ℓ is a functor since morphisms of abelian varieties preserve torsion.

In characteristic p we have the Frobenius morphism which sends a point x to x^q (raise each coordinate to the q^{th} power). Call this map π_X. The action of π_X on X passes by functoriality to an action on $V_\ell(X)$ as a $\mathbb{Q}_\ell$-linear map. Let $f_X(T)$ denote the characteristic polynomial of $V_\ell(\pi_X)$ on $V_\ell(X)$. Our point of departure is from two fundamental results of Tate and Honda. From now on let k be the field $\mathbb{F}_q$.

Definition: If A and B are abelian varieties defined over k, then a morphism $q: A \to B$ is called an isogeny if q is surjective and has a finite kernel.

It is a fact that if $\phi: B \to A$ is an isogeny, then there exists an isogeny $\Psi: B \to A$ (Waterhouse and Milne [25], p.54). Therefore, the relation of isogeny is an equivalence relation on the set of abelian varieties over k. The equivalence classes are called isogeny classes.

If $\bar{k}$ is an algebraic closure of k and $\mathbb{G}$ is the Galois group of $\bar{k}/k$, then $V_\ell X$ inherits a $\mathbb{G}$-action, since the elements of $\mathbb{G}$ preserve torsion. By functoriality of V_ℓ there exists a map

$$\mathrm{Hom}(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{G}}(V_\ell A, V_\ell B) .$$

Tate's theorem (Tate [22]) states that this map is a bijection. Tate's theorem allows us to connect the Frobenius action on $V_\ell(X)$ with the zeta function of X because of the

Corollary: (Tate [22], Waterhouse and Milne [25]). If A and B are abelian varieties over k, then the following

are equivalent:

(1) A is isogenous to B.

(2) $V_\ell A$ is isomorphic, as a $\mathbb{G}$-module, to $V_\ell B$ for some $\ell \neq p$.

(3) $f_A(T) = f_B(T)$.

(4) $Z(A,T) = Z(B,T)$.

The zeta function $Z(A,T)$ is related to the characteristic polynomial $f_A(T)$ through the fixed points of the Frobenius. Consider $\pi_A - 1_A : A \to A$. N_s, the number of $\mathbb{F}_{q^s}$ - rational points of A, equals the number of points of the kernel of $\pi_A^s - 1_A$. If we can describe $\deg(\pi_A^s - 1_A)$, the degree of the map $\pi_A^s - 1_A$, for all s, we will recover $Z(A,T)$. The remarkable fact that allows us to do this is

Proposition: (Mumford [14]). $\deg(\pi_A - 1_A) = f_A(1) = \prod_i (1-\alpha_i)$ where α_i are the complex roots of $f_A(T)$. More generally, $\deg(\pi_A^s - 1_A) = \prod_i (1-\alpha_i^s)$.

We see that the roots of $f_A(T) = 0$, which are the eigenvalues of $V_\ell(\pi_A)$, determine N_s for $s=1,2,\ldots$. This sequence, in turn, determines $Z(A,T)$. Conversely, $Z(A,T)$ determines the set $\{N_s\}$ which gives the numbers $\prod_i (1-\alpha_i^s)$. It is then seen that the values $\prod_i (1-\alpha_i^s)$ for finitely many s determine the set $\{\alpha_i\}$.

An abelian variety A is called elementary or simple if A has no nontrivial subvarieties.

Proposition. (Weil [26], Mumford [14]). Let A be elementary over k. $\mathrm{End}(A)$ denotes the ring of endomorphisms of A,

$\mathrm{End}^\circ(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then $\mathrm{End}^\circ(A)$ is a division algebra with center $\mathbb{Q}(\pi_A)$. Every embedding of $\mathbb{Q}(\pi_A)$ in $\mathbb{C}$ has absolute value $|\pi_A| = q^{\frac{1}{2}}$. If λ is a root of $f_A(T)$, then $|\lambda| = q^{\frac{1}{2}}$. $f_A(T)$ is of the form $m_A(T)^n$ where $m_A(T)$ is monic, defined over $\mathbb{Z}$ and irreducible over $\mathbb{Q}$. Hence a root of $f_A(T)$ is an algebraic integer.

Definition: An algebraic integer w is called a q-Weil number if $|w| = q^{\frac{1}{2}}$ in any complex embedding, where q is a power of a prime p .

What we have seen so far is that for A elementary, π_A determines $f_A(T)$ which determines a conjugacy class of q-Weil numbers. Tate's theorem tells us that any abelian variety over k which is isogenous to A determines the same conjugacy class of Weil numbers. Conversely, if two elementary abelian varieties determine the same conjugacy class of q-Weil numbers, Tate's theorem implies that they are isogenous. Hence we have a map Φ_q from the set of k-isogeny classes of k-elementary abelian varieties to the set of conjugacy classes of q-Weil numbers, and Tate's theorem implies that this map is injective. Furthermore, we have

Theorem: (Honda [7], Tate [23]). Given a conjugacy class $\{w_i\}$ of q-Weil numbers, there exists an isogeny class I of k-elementary abelian varieties such that if $A \in I$, then $f_A(T)$ has precisely the set $\{w_i\}$ as its roots.

We see immediately that this theorem, together with the above remarks, gives us a one-to-one correspondence between the set of k-elementary abelian varieties and conjugacy classes

of q-Weil numbers.

We would like to briefly sketch Honda's proof of the last theorem in order to motivate our problem. Our reference here is Honda's paper [7]. Honda works not only with Weil numbers, but with what he calls ideals of type (A_o). These are ideals I in a suitable ring of algebraic integers having the property that $I^{\sigma} I^{\sigma\rho} = (p^a)$ where I^{σ} is a conjugate of I and ρ is complex conjugation. We will call these Weil ideals, the analogy with Weil numbers being clear. Let $\bar{k}$ denote an algebraic closure of $k=\mathbf{F}_q$, where $q=p^a$. If w_1 and w_2 are q-Weil numbers, say that w_1 is equivalent to w_2, $w_1 \sim w_2$, if $w_1^{n_1}$ is conjugate to $w_2^{n_2}$ for some positive integers n_1 and n_2. Note that if w is a q-Weil number, and ζ is an Nth root of unity, then $w \sim \zeta w$. The same definition applies to Weil ideals. We have maps Φ: {$\bar{k}$-isogeny classes of $\bar{k}$-simple abelian varieties over $\bar{k}$} $\rightarrow$ {equivalence classes of q-Weil numbers and Φ_q: {k-isogeny classes of k-simple abelian varieties over k} $\rightarrow$ {conjugacy classes of q-Weil numbers}.

Honda proves that Φ is surjective. The surjectivity of the map Φ_q follows from that of Φ by a descent argument.

An important part of Honda's proof is understanding the relationship between Weil numbers and Weil ideals. It is clear that any Weil number generates a Weil ideal. It is not so clear that the converse is true, i.e., that any Weil ideal is generated by a Weil number (Honda, Th.1). Thus, there is a bijective correspondence between {equivalence classes of

q-Weil numbers} and {equivalence classes of q-Weil ideals}. Honda also proves (Honda [ ], Th. 2, p. 87)

Proposition: Given a Weil ideal I, there is a CM-type $(F,\{\phi_i\})$ such that

(a) F is a CM-field normal over $\mathbb{Q}$

(b) For a prime divisor P of p in F,

we have

$$I \sim \prod_i P^{\Psi_i}$$

where $\Psi_i=\phi_i^{-1}$. For definition and facts about CM-types, CM-fields, etc., see Shimura-Taniyama [20], and Lang [11]. Once a CM-type is associated to a Weil ideal I, Shimura-Taniyama tells us that we can associate an abelian variety defined over an algebraic number field having that CM-type (Shimura-Taniyama [20], Theorems 2 and 3, p.45-46). Honda then reduces this abelian variety at a prime divisor of p in F, and shows that the CM-type can be chosen so the reduction is simple and has Frobenius element which generates the equivalence class of I.

Once the surjectivity of Φ has been proven, the surjectivity of Φ_q is shown by using a descent argument that runs as follows. If w is a q-Weil number, let $I = (w)$ be the associated q-Weil ideal. Then there is a CM-type $(F,\{\phi_i\})$ and a prime P lying above p such that if B is an abelian variety of type $(F,\{\phi_i\})$, and $\bar{B}$ is B reduced at P, there is $w_o \in F$ which gives the Frobenius endomorphism of $\bar{B}$. w_o may not equal w, but $w_o \sim w$, so there exists an integer ν such that w_o^ν is conjugate to w^ν.

Base change the ground field of B to $\mathbb{F}_{q^\nu}$ and let $A = B \otimes_{\mathbb{F}_q} \mathbb{F}_{q^\nu}$. There is an imbedding of $\mathbb{Q}(w^\nu)$ into $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ mapping w^ν to the Frobenius endomorphism of A. This observation reduces the surjectivity problem to a descent problem for a finite extension. Honda applies the norm construction (Weil [28], or next section) to A relative to the field extension $\mathbb{F}_{q^\nu}/\mathbb{F}_q$. This descends the field of definition to $\mathbb{F}_q$. Honda then shows that w appears as a characteristic root of Frobenius acting on the norm. In fact, w multiplied by all the νth roots of unity occur as characteristic roots. Our first problem is to describe the isomorphism classes of these other "twisted" Weil-numbers relative to the isogeny type determined by w.

Chapter 1

Multiplying Weil Numbers by Roots of Unity

Let w be a q-Weil number for the k-elementary abelian variety A and let ζ be an N^{th}-root of unity. ζw satisfies $|\zeta w| = |w| = q^{\frac{1}{2}}$. Therefore, by Honda's theorem, w determines an isogeny class of a k-elementary abelian variety. Our problem is to explicitly describe this isogeny class. We first briefly review an algebraic-geometric construction called descending the field of definition or norm (Weil [27],[28]; Grothendieck [5]). Given a morphism of rings $R \to S$, we can map R-schemes to S-schemes by taking the pullback along $\mathrm{Spec}S \to \mathrm{Spec}R$. This operation is functorial. We will denote it by $\_ \otimes_R S$ and call it base change. The norm functor, written $N_{S/R}$, is the right adjoint to base change (if this adjoint exists). That is, if Y is an R-scheme and X is an S-scheme, there is a natural (in X and Y) bijective correspondence.

$\mathrm{Hom}_S(Y \otimes_R S, X) \simeq \mathrm{Hom}_R(Y, N_{S/R}X)$. Grothendieck [5] has shown that the norm exists if $R \to S$ is flat and proper. In particular, the norm exists if $R \to S$ is a field extension.

Proposition 1. If k'/k is an extension of finite fields of degree N and X is an abelian variety defined over k', then $N_{k'/k}X$ is an abelian variety defined over k and

$$(N_{k'/k}X) \otimes_k k' \simeq \prod_i X^{g_i}$$

where $G = \{g_1, \ldots, g_N\}$ is the Galois group of k'/k and X^{g_i} is the pullback of X along the automorphism

$g_i : k' \longrightarrow k'$.

Proof: Let $Y = N_{k'/k}X$ in the above adjointness relation; $\mathrm{Hom}_{k'}(N_{k'/k}X \otimes_k k', X) \tilde{=} \mathrm{Hom}_k(N_{k'/k}X, N_{k'/k}X)$. Taking the preimage of $\mathrm{id}_{N_{k'/k}X}$ by this bijection gives a morphism $N_{k'/k}X \otimes_k k' \to X$. By naturality, this morphism has the universal property that if Z is a variety over k and $Z \otimes_k k' \to X$ is a morphism over k' , there exists a unique morphism $Z \to N_{k'/k}X$ such that $A \otimes_k k' \to N_{k'/k}X \otimes_k k'$ yields the following commutative diagram:

$$\begin{array}{ccc} (N_{k'/k}X) \otimes_k k' & \longrightarrow & X \\ & \nwarrow \quad \nearrow & \\ & Z \otimes k' & \end{array} \quad .$$

This property characterizes the functor $N_{k'/k}$ uniquely upto isomorphism. Since k'/k is Galois, we have by the normal basis theorem, $k' \otimes_k k' \xrightarrow{\tilde{}} \pi_i k'$ indexed over the number of elements of G . Therefore we have the following commutative diagram of spectra

$$\begin{array}{ccccc} \mathrm{Spec}(\pi k') \cong \mathrm{Spec}(k' \otimes_k k') & \longrightarrow & \mathrm{Spec}\, k' \\ \downarrow & & \downarrow \\ \mathrm{Spec}\, k' & \longrightarrow & \mathrm{Spec}\, k \end{array} \quad .$$

By pulling back, we get the following commutative diagram

$$\begin{array}{ccc} \pi_i X & \xrightarrow{g_i} & X \\ \downarrow & & \downarrow \\ \mathrm{Spec}(k' \otimes_k k') & \longrightarrow & \mathrm{Spec}(k') \end{array}$$

It is then an easy diagram chase to verify that the map $\pi_i X \xrightarrow{g_i} X$ satisfies the required universal property.

Now let A be a k-elementary abelian variety in the isogency class determined by w. We form another abelian variety as follows. If ζ is an N^{th} root of unity, let k'/k be the extension of degree N. Raise the field of definition of A to k'; let $A' = A \otimes_k k'$. Lower the field of definition by taking the norm down to k; let $B = N_{k'/k}A'$. We compare the characteristic polynomials $f_B, f_{A'}$ of the Frobenii acting on B and A' respectively. Since B becomes isomorphic to the N-fold product A'^N over k', the dimension of B equals $N\cdot(\dim A)$. Hence the degree of the polynomial $f_B(T)$ is $2N\cdot(\dim A)$ (Mumford [ ]). Consider the polynomial $f_{A'}(T^N)$. Its degree is also $2N\cdot(\dim A)$.

Proposition 2. $f_B(T) = f_{A'}(T^N)$.

Proof: These are both monic and defined over $\mathbb{Z}$. We show that they have the same roots. Let r be a root of $f_B(T)$, i.e., an eigenvalue of Frobenius acting on $V_\ell(B)$ for some prime ℓ, $\ell \neq p$. $B \otimes_r k' \simeq (A')^N$ implies that r^N is a root of $f_{(A')^N}(T)$. This is because after base change by a field extension of degree N, the new Frobenius is the old one iterated N times. But by the correspondence between factoring of isogeny type and characteristic polynomials, $f_{(A')^N}(T) = (f_{A'}(T))^N$. Therefore, r^N is a root of

$f_{A'}(T)$, i.e., r is a root of $f_{A'}(T^N)$. So every root of $f_B(T)$ is a root of $f_{A'}(T^N)$. But we have already checked that these have the same degree. This finishes the proof.

Now consider the Weil number ζw . By Proposition 2, $f_B(\zeta W) = f_{A'}(\zeta^N w^N) = f_{A'}(w^N) = 0$. Therefore, the conjugacy class of ζw determines a k-elementary subvariety of B . In fact, Proposition 2 shows that any N^{th} root of unity times any Weil number for A determines a k-elementary subvariety of B .

Our next task is to analyze the k-isogeny type of B . To do this we utilize the formalism of k'/k-forms (see Milne [12], pg. 183). Fix the abelian variety A over k . A k'/k-<u>form</u> for A is a pair (C,Ψ) where C is an abelian variety over k and $\Psi : A \otimes_k k' \to C \otimes_k k'$ is an isomorphism defined over k' . Let $Aut_{k'}(A)$ be the automorphisms of A defined over k' , and let G be the Galois group of k'/k . Then (C,Ψ) determines a 1-cocycle in the sense of cohomology of groups $G \to Aut_{k'}(A)$ by sending $g \mapsto \Psi^{-1}\Psi^g$, where $\Psi^g = g\Psi g^{-1}$. In this expression g^{-1} acts on $A \otimes_r k'$ through its action on k' , and g acts on $C \otimes_k k'$ through its action on k' . It is a basic fact of group cohomology (see e.g. Serre [19]) that this correspondence sets up a bijection between $H^1(G,Aut_{k'},A)$ and the isomorphism classes of k'/k-forms for A .

We will use a different formulation of k'/k-forms. Our reference here is Milne [12], pg. 183. Let R be a commutative subring of $End_k(A)$, the endomorphisms of A

defined over k, and M an R-free G-module. Let $\eta: R^n \xrightarrow{\sim} M$ be an R-isomorphism. Define a 1-cocycle $G \to G\ell_n(R)$ by the rule $g \to \eta^{-1} g \eta g^{-1} = \eta^{-1} \eta^g$. Note that since G acts trivially on R, $\eta^{-1} g \eta g^{-1} = \eta^{-1} g \eta$ as an element of $G\ell_n(R)$ acting on R^n. Regard $G\ell_n(R)$ as a subgroup of $\mathrm{Aut}_{k'}(A^n)$ to get a 1-cocycle $G \to \mathrm{Aut}_{k'}(A^n)$, hence an element of $H^1(G, \mathrm{Aut}_{k'}(A^n))$ i.e. a k'/k-form for A^n. Let $(M \otimes_R A, \Psi_A)$ denote the k'/k form so induced. We wish to describe this construction functorially.

Let M, M' be R-free G-modules with R-ranks n, n' respectively, i.e., there are isomorphisms $\eta: R^n \to M$ and $\eta': R^{n'} \to M'$. Let $\phi: M \to M'$ be a morphism of G-modules. By definition there are associated k'/k-forms $(M \otimes_R A, \Psi_A)$ and $(M' \otimes_R A, \Psi'_A)$ for powers of A. Define a map

$$\phi_{Ak'}: (M \otimes_R A) \otimes_k k' \longrightarrow (M' \otimes_R A) \otimes_k k'$$

over k' in such a way that the following diagram commutes:

$$\begin{array}{ccc} A^n \otimes k' & \xrightarrow{\Psi_A} & (M \otimes_R A) \otimes 1' \\ \Big\downarrow{\scriptstyle \eta^{-1}\phi\eta} & & \Big\downarrow{\scriptstyle \phi_{Ak'}} \\ A^{n'} \otimes k' & \xrightarrow{\Psi'_A} & (M' \otimes_R A) \otimes k' \end{array}$$

To show the functoriality of the $\_\_ \otimes_R A$ construction, we need to show that $\phi_{Ak'}$ descends to a morphism $\phi_A: M \otimes_R A \to M' \otimes_R A$ over k. To do this, it suffices to show that $\phi_{Ak'}$ preserves descent data for $M \otimes_R A$ (see Waterhouse [24], pg. 132, paragraph 1). To illustrate, we argue with the module analogy.

Let N,N' be k-modules, (F,Ψ) a k'/k-form for N, (F',Ψ') a k'/k-form for N' and consider

$$\begin{array}{ccc} N \otimes k' & \xrightarrow{\Psi} & F \otimes k' \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle \Psi'\Psi^{-1}} \\ N' \otimes k' & \xrightarrow{\Psi'} & F' \otimes k' \end{array}$$

where T is defined over k. We wish to show that $\Psi' T \Psi^{-1}$ preserves descent data, hence descends to a map $F \to F'$ over k.

$N \otimes k'$ has canonical descent data Π_N, i.e.,

$$\Pi_N : N \otimes k' \otimes k' \longrightarrow N \otimes k' \otimes k'$$

$$n \otimes a \otimes b \longmapsto n \otimes b \otimes a \quad \text{(interchange)}$$

Let $n \otimes a \in N \otimes k'$. $\Psi(n \otimes a) = \Psi(n \otimes 1) \cdot a$

$$= (\Sigma f_i \otimes s_i)a = \Sigma f_i \otimes s_i a \,, \quad f_i \in F \,, \quad s_i \in k' \,.$$

On $N \otimes k' \otimes k'$ we have

$$\Psi \otimes id : N \otimes k' \otimes k' \longrightarrow F \otimes k' \otimes k'$$

$$n \otimes a \otimes b \longrightarrow \Psi(n \otimes a) \otimes b = \Sigma f_i \otimes s_i a \otimes b$$

or

$$(\Psi \otimes id)_t : N \otimes k' \otimes k' \longrightarrow F \otimes k' \otimes k'$$

$$n \otimes a \otimes b \longmapsto \Sigma f_i \otimes a \otimes s_i b$$

(t stands for "twist"). If Θ_F is the canonical descent data for F, we wish to check whether $(\Psi \otimes id)^{-1} \Theta_F (\Psi \otimes id)_t$ defines descent data for N.

But

$$(\Psi^{-1} \otimes \mathrm{id})\ \Theta_F(\Psi \otimes \mathrm{id})_t\ (n \otimes a \otimes b)$$

$$= (\Psi^{-1} \otimes \mathrm{id})\ \Theta_F(\Sigma f_i \otimes a \otimes s_i b)$$

$$= (\Psi^{-1} \otimes \mathrm{id})(\Sigma f_i \otimes s_i b \otimes a)$$

$$= \Psi^{-1}(\Sigma f_i \otimes s_i b) \otimes a = n \otimes b \otimes a\ ,$$

which is the "interchange" descent data for N. Observe that we get the same thing if we take

$$(\Psi \otimes \mathrm{id})_t^{-1}\ \Theta_F(\Psi \otimes \mathrm{id}) \quad \text{instead.}$$

That is, $(\Psi \otimes \mathrm{id})_t^{-1}\ \Theta_F(\Psi \otimes \mathrm{id})(n \otimes a \otimes b)$

$$= (\Psi \otimes \mathrm{id})_t^{-1}\ \Theta_F(\Sigma f_i \otimes s_i a \otimes b)$$

$$= (\Psi \otimes \mathrm{id})_t^{-1}\ (\Sigma f_i \otimes b \otimes s_i a) = n \otimes b \otimes a\ .$$

Going back to our diagram, we can now show that $\Psi' T \Psi^{-1}$ preserves descent data

$$(\Psi' T \Psi^{-1} \otimes \mathrm{id})(\Psi \otimes \mathrm{id})\ \Theta_N(\Psi \otimes \mathrm{id})_t^{-1}$$

$$= (\Psi' T \otimes \mathrm{id})(\Psi^{-1} \otimes \mathrm{id})(\Psi \otimes \mathrm{id})\ \Theta_N(\Psi \otimes \mathrm{id})_t^{-1}$$

$$= (\Psi' T \otimes \mathrm{id})\ \Theta_N(\Psi \otimes \mathrm{id})_t^{-1} = (\Psi' \otimes \mathrm{id})(T \otimes \mathrm{id})\ \Theta_N(\Psi \otimes \mathrm{id})_t^{-1}$$

$$= (\Psi' \otimes \mathrm{id})\ \Theta_N(T \otimes \mathrm{id})(\Psi \otimes \mathrm{id})_t^{-1} \quad \text{(since } T \text{ preserves descent data)}$$

$$= (\Psi' \otimes \mathrm{id})\ \Theta_N(\Psi'^{-1} \otimes \mathrm{id})(\Psi' \otimes \mathrm{id})(T \otimes \mathrm{id})(\Psi \otimes \mathrm{id})_t^{-1}$$

$$= (\Psi' \otimes \mathrm{id})_t\ \Theta_N(\Psi'^{-1} \otimes \mathrm{id})(\Psi' \otimes \mathrm{id})(T \otimes \mathrm{id})(\Psi \otimes \mathrm{id})^{-1} \quad \text{(by previous observation)}$$

$$= (\Psi' \otimes \mathrm{id})_t\ \Theta_N(\Psi'^{-1} \otimes \mathrm{id})(\Psi' T \Psi^{-1} \otimes \mathrm{id})\ .$$

This shows that $\Psi' T \Psi^{-1}$ commutes with descent data. Hence the "tensor product" construction $\_ \otimes_R A$ yields a functor

from the category of R-free G-modules to the category of k'/k-forms for powers of A .

Now form the group ring R[G] . This is clearly an R-free G-module. Recall that $A' = A \otimes_r k'$.

Proposition 3.: $R[G] \otimes_R A = N_{k'/k}A'$.

We know that $R[G] \otimes_R A$ is a k'/k-form for A^N determined by a representation $G \to \mathrm{Aut}(A')$ for A^N , and can also be described as a G-representation. We compare these representations. If they are equal, then Proposition 2 will follow.

We first review another way of constructing $N_{k'/k}A'$ which allows us to see the relationship with G-representations. Let $C = \prod_i (A')^{g_i}$. Let g be the canonical generator of G , the Galois group of k'/k . Then g induces a k'-isomorphism

$$t_g : C \to C^g$$

by permutation of factors according to g . We then have maps

$$C^g \xrightarrow{t_{g^2}} C^{g^2} \longrightarrow \cdots \longrightarrow C^{g^{n-1}} \xrightarrow{t_{g^N}} C^{g^N} = C .$$

It is clear that $t_{g^N} \circ t_{g^{N-1}} \circ \cdots \circ t_{g^2} \circ t_g = id_C$. For $2i \leq j \leq N$, let

$$f_{ij} = t_{g^j} \circ \cdots \circ t_{g^i} : C^{g^{i-1}} \longrightarrow C^{g^j}$$

and $f_{ij} = f_{ji}^{-1}$. Then we have

$$f_{ij} \circ f_{jk} = f_{ik}$$

$$f_{i+j,i+k} = f_{j,k}^{t_{g^i}} .$$

These are precisely the conditions required to descend the field of definition (Weil [ ]), and by our particular choice of f_{ij}'s , we get the norm construction up to isomorphism (Honda [7], pg.89-90). To go from this description to the G-representation, we reason as follows. $(A')^{g^i}$ is A' pulled back along g^i , i.e. we have

$$\begin{array}{ccc} (A')^{g^i} & \longrightarrow & A' \\ \downarrow & & \downarrow \\ k' & \xrightarrow{g^i} & k' \end{array} .$$

Since g^i is an automorphism, the top map is an isomorphism. This gives isomorphisms $\alpha_i : A' \to (A')^{g^i}$, $i=1,\ldots,N$, hence an isomorphism $\alpha = \Pi\alpha_i : \Pi A' \to \prod_i (A')^{g^i}$.

This induces a G-action on A' by

$$\Pi A' \xrightarrow{\alpha} \prod_i (A')^{g^i} \xrightarrow{t_g} \prod (A')^{g^i} \xrightarrow{\alpha^{-1}} \Pi A' .$$

It is easily seen that $g \in G$ acts on points of $\Pi A'$ according to how g permutes the factors in $\prod_i (A')^{g_i}$.

Hence the G-representation induced by $N_{k'/k}A'$ is the same as that induced by $R[G] \otimes_R A$. This proves Proposition 3.

Now assume that $R = End(A)$ is commutative and that all the endomorphisms of A are defined over k and that A is k-simple. We want to compare the categories of R-free G-modules and k'/k-forms for powers of A . Let M denote the category of R-free G-modules and F the category of k'/k-forms for powers of A . We have seen that $\_\_\otimes_R A$ is a functor $M \to F$.

Theorem 1. $\_\_\otimes_R A$ induces an equivalence of categories.

Proof: Let (B,Ψ) be a k'/k-form for A^n. (B,Ψ) corresponds to the 1-cocycle $G \to \mathrm{Aut}(A^n)$ which sends $g \in G$ to $\Psi^{-1}\Psi^g$. Recall that A was assumed to be k-elementary, so an endomorphism of A^n is an element of the algebra of $n \times n$ matrices with entries in $R = \mathrm{End}(A)$. In particular, an automorphism is in $G\ell_n(R)$. Hence, $\mathrm{Aut}(A^n) = G\ell_n(R)$. Let M be R^n with G-action $G \to G\ell_n(R)$ given by $g \to \Psi^{-1}\Psi^g$. Then it is clear from the definition of the functor $\_\_\otimes_R A$ that $M \otimes_R A \tilde{=} (B,\Psi)$. Hence, $\_\_\otimes_R A$ maps onto the objects of F.

To prove that $\_\_\otimes_R A$ is full and faithful, let (B,Ψ) and (B_1,Ψ_1) be k'/k-forms for A^n and A^{n_1} respectively. and let $\phi: (B,\Psi) \to (B_1,\Psi_1)$ be a morphism. Over k' we have a diagram

$$\begin{array}{ccc} (A')^n & \xrightarrow[\tilde{=}]{\Psi} & B \otimes_r k' \\ {\scriptstyle \Psi_1^{-1}\,\phi_{k'},\Psi}\ \vdots & & \Big\downarrow {\scriptstyle \phi k'} \\ (A')^{n_1} & \xrightarrow[\tilde{=}]{\Psi_1} & B_1 \otimes_r k' \end{array}$$

where the dotted arrow is filled in to make the diagram commute. Let M and M_1 be R-free G-modules such that $M \otimes_R A = (B,\Psi)$ and $M_1 \otimes_R A = (B_1,\Psi_1)$. $\Psi_1^{-1}\,\phi_{k'},\Psi: M \to M_1$. We check that this map preserves G-action. G acts on M by $g \cdot m = (\Psi^{-1}g\Psi)m, g \in G, m \in M$, where $\Psi^{-1}g\Psi$ has matrix representation as an $n \times n$ matrix with entries in R. Similarly, G

acts on M_1 by $gm_1 = (\Psi_1^{-1}\, g\Psi_1)m_1$. Therefore,

$$(\Psi_1^{-1}\ \phi_{k'},\Psi)(gX) = \Psi_1^{-1}\ \phi_{k'},\ \Psi\Psi^{-1}g\Psi x$$

$$= (\Psi_1^{-1}\ \phi_{k'},g\ \Psi)(x)$$

$$g\cdot(\Psi_1^{-1}\ \phi_{k'},\Psi)(x) = (\Psi_1^{-1}\ g\ \Psi_1\Psi_1^{-1}\ \phi_{k'},\Psi)(x)$$

$$= (\Psi_1^{-1}\ g\ \phi_{k'},\Psi)(x)$$

for $g\varepsilon G$, $x\varepsilon M$.

But $\phi_{k'}\cdot g = g\cdot\phi_{k'}$, since $\phi_{k'}$ is obtained by tensoring with k' over k . Therefore, $\Psi_1^{-1}\ \phi_{k'},\Psi$ preserves G-action. It is clear from the definition of the functor $\_\otimes_R A$ that the morphism $\Psi_1^{-1}\phi_{k'},\Psi\colon M \to M'$ gets sent to ϕ . This shows that $\_\otimes_R A$ is full. It is easy to check that it is faithful. This finishes the proof of Theorem 1.

We now return to the problem of describing the isogeny type of $B = N_{k'/k}A'$. By Proposition 2 we have a description of B as $R[G]\otimes_R A$. Since G is the Galois group of the finite extension k'/k of finite fields, we have $R[G] \simeq R[X]/(X^N - 1)$. The polynomial X^N-1 factors over $R^o = \mathrm{End}(A)\otimes_{\mathbb{Z}} \mathbb{Q}$ depending on the N^{th} roots of unity which lie in R . Write this factorization as

$$X^N - 1 = \prod_i P_i(X) .$$

The polynomials $P_i(x)$ are relatively prime and irreducible over R^o. Therefore we have

$$R^o[G] \simeq R^o[X]/(\pi P_i(X))$$

$$\simeq \prod_i (R^o[X]/(P_i(X))$$

using the Chinese Remainder Theorem. Recall that the functor $\_ \otimes_R A$ is product preserving. Therefore,

$$B \tilde{=} R[G] \otimes_R A \text{ is isogenous to } \prod_i ((R[X]/(P_i(X))) \otimes_R A) .$$

We must verify that this gives the complete isogeny factorization.

Proposition 4. Notation as above. $\frac{R(X)}{(P_i(X))} \otimes_R A$ is k-elementary.

Proof: It suffices to prove that $End^\circ(R[X]/P_i(X)) \otimes_R A)$ is a division algebra. By Theorem 1,

$$End^\circ(\frac{R[X]}{P_i(X)} \otimes_R A) = End(R[X]/P_i(X)) \otimes_R A) \otimes_Z \mathbb{Q}$$

is isomorphic to $End_G(\frac{R[X]}{(P_i(X))}) \otimes_Z Q$.

Therefore, we wish to show that $End_G(\frac{R[X]}{(P_i(X))}) \otimes_Z Q$ is a division algebra.

We first remark what the G-action looks like on $R[X]/P_i(X)$. Under the isomorphism

$$R[G] \xrightarrow{\tilde{}} R[X]/(X^N-1) ,$$

the action of the canonical generator g on G passes to multiplication by X . Under the isomorphism

$$R[X]/(X^N-1) \xrightarrow{\tilde{}} \prod_i R[X]/(P_i(X))$$

X breaks into say r components $(X_1,\ldots,X_r)$. So the action of g on the i^{th} component $R[X]/(P_i(X))$ is multiplication by X_i which is the coset represented by X . Hence, $End_G(R[X]/P_i(X))$ consists of all additive functions

f from $R[X]/P_i(X)$ to itself having the property that $f(X\cdot g) = X\cdot f(g)$ where $g\in R[X]/(P_i(X))$. In particular, multiplication by elements of $R[X]/(P_i(X)$ has this property, i.e.,

$$R[X]_{/(P_i(X))} \hookrightarrow \mathrm{End}_G(R[X]_{/(P_i(X)}) \ .$$

We wish to show that this inclusion is an equality. Therefore, let $f\in \mathrm{End}_G(R[X]/(P_i(X))$. Then, $f(x) = X\cdot f(1)$, so that

$$\begin{aligned} & f(a_nX^n + a_{n-1}X^{n-1} + \ldots + a_iX + a_o) \\ &= f(a_nX^n) + f(a_{n-1}X^{n-1}) + \ldots + f(a_iX) + f(a_o) \\ &= f(a_n)X^n + f(a_{n-1})X^{n-1} + \ldots + f(a_i)X + f(a_o) \end{aligned}$$

where the a_i's are elements of R . But by definition, f is also a map of R-modules, hence $f(a_i) = a_i\cdot f(1)$. Therefore, the last expression becomes

$$(a_nX^n + a_{n-1}X^{n-1}) + \ldots + a_1X + a_o)\cdot f(1) \ ,$$

i.e., f is multiplication by $f(1)$. Therefore,

$$\mathrm{End}_G(R[X]/P_i(X)) = R[X]/(P_i(X)) \ .$$

Tensoring with Q gives

$$\mathrm{End}_G(R[X]/P_i(x)) \otimes_Z Q = R[X]/(P_i(x)) \otimes_Z Q \ .$$

But $R[X]/(P_i(X)) \otimes_Z Q$ is a division algebra because $P_i(X)$ is irreducible over R .

Next we produce examples of k'/k-forms corresponding to multiplying Weil numbers by -1 . We do this for hyperelliptic curves. We first treat the case of elliptic curves, using an argument of Baldisserri [ ].

Let $E_1: Y^2 = 4x^3 - ax - b$

$E : Y^2 = 4x^3 - au^2x - bu^3$

be elliptic curves defined over $k = \mathbf{F}_q$. Let N_1 and N be the number of rational points of E_1 and E respectively. Note that

$$N = 1 + \sum_{x \in k} \left[1 + \left(\frac{4x^3-au^2x-bu^3}{q}\right) \right]$$

$$= q+1 + \sum_{x \in k} \left(\frac{4x^3-au^2x - bu^3}{q}\right)$$

where $\left(\frac{\cdot}{q}\right)$ is the Legendre symbol:

$$\left(\frac{x}{q}\right) = \begin{cases} +1 & \text{if } x \text{ is a square in } k \\ -1 & \text{if } x \text{ is not a square in } k \\ 0 & \text{if } x=0 . \end{cases}$$

Letting $\phi_q(u) = \sum_{x \in \mathbf{F}_q} \left(\frac{4x^3-au^2x-bu^3}{q}\right)$, we have

$$N = q+1 + \phi_q(n) .$$

Make the change of variables $x=uz$ to get

$$\phi_q(u) = \sum_{z \in k} \left(\frac{4u^3 z^3 - au^2uz - bu^3}{q}\right)$$

$$= \sum_{z \in k} \left(\frac{4z^3 - az - b}{q} \right) \left(\frac{u^3}{q} \right)$$

$$= \left(\frac{u}{q} \right) \phi_q(1) \ .$$

Therefore, we have

$$N = q+1 + \left(\frac{u}{q}\right) \phi_q(1) \ .$$

But $\phi_q(1)$ is also equal to $N_1 - q - 1$, so we get

$$N = q+1 + \left(\frac{u}{q}\right)(N_1 - q - 1)$$

$$= (q+1)\left(1 - \left(\frac{u}{q}\right)\right) + \left(\frac{u}{q}\right) N_1 \ .$$

If $u = -1$ and $\left(\frac{-1}{q}\right) = +1$, then $N = N_1$ and E and E_1 have the same zeta function. If -1 is not a square in k, then $\left(\frac{u}{q}\right) = -1$, so we get

$$N = 2(q+1) - N_1$$

$$= (q+1) + (q+1-N_1) \ , \text{ i.e.,}$$

$N - (q+1) = q+1 - N_1$. Therefore, if α is a root of the zeta function for E, we get

$$\alpha + \bar{\alpha} = q+1 - N$$

$$= -(q+1) + N_1 \ .$$

On the other hand,

$$N_1 = q+1 - (\alpha_1 + \bar{\alpha}_1)$$

where α_1 is a root of the zeta function for E_1. Therefore,

$$\alpha+\bar{\alpha} = -(\alpha_1+\bar{\alpha}_1) ,$$

i.e., $\mathrm{Re}(\alpha) = \mathrm{Re}(-\alpha_1)$.

But by the Riemann hypothesis,

$$\alpha\bar{\alpha} = q = \alpha_1\bar{\alpha}_1$$

which implies that $\mathrm{Im}(\alpha) = \mathrm{Im}(\alpha_1)$ or $\mathrm{Im}(-\bar{\alpha}_1)$.

We sum this up in

Proposition 5.: Notation as above. If w is a Weil number of the elliptic curve $E_1: Y^2 = 4x^3+ax+b$ over k , then the elliptic curve E with equation $Y^2 = 4x^3+au^2+bu^3$, where $u\in k$ is such that $(\frac{u}{q}) = -1$ has Weil number $-w$. E is a k'/k-form for E_1 where k' is the quadratic extension of k .

Proof: The first sentence has been proven above. To prove the second sentence, let $t = u$ and $k'=k(t)$. Define a morphism $E_1 \to E$ by sending $(x,y) \dashrightarrow (t^2x,t^3y)$. It is easily seen that this is an isomorphism defined over k' .

We now generalize this argument to hyperelliptic curves.

Definition: A hyperelliptic curve is a curve X which admits a degree 2 surjective rational function $f: X \to \mathbb{P}^1$ where $\mathbb{P}^1$ is the projective line. We take our hyperelliptic curves to be defined over $k=\mathbb{F}_q$, $q=p^a$, $p\neq 2$.

Lemma 1: We can put the equation of a hyperelliptic curve C defined over k into the form

$$Y^2 = X(X-1)(X-\lambda_1) \ldots (X-\lambda_s)$$

where, if g = genus of C , $s= 2g-2$, and $\lambda_i\in\bar{k}$,.an algebraic closure of k .

Proof: (Springer [21]). We rewrite Springer's argument, being careful that the argument goes through in finite characteristic. Let $K(C)$ and $K(\mathbb{P}^1)$ denote the function fields of C and $\mathbb{P}^1$. $K(\mathbb{P}^1) = \bar{k}(X)$ where $\bar{k}$ is an algebraic closure of k, and $\bar{k}(X) \subset K(C)$. $K(C)$ is a quadratic extension of $\bar{k}(X)$. C comes equipped with a rational function $f: C \to \mathbb{P}^1$, $f \in K(C)$. Hence, f satisfies a quadratic equation $f^2 + R_1(x)f + R_2(X) = 0$, $R_1(X), R_2(X) \in \bar{k}(X)$. Make the change of variable

$$u = f + \frac{R_1(X)}{2} .$$

Then u satisfies $u^2 = -R_2(X) + \frac{R_1(X)}{4}$. Since $\bar{k}$ is algebraically closed, we can write

$$u^2 = \frac{(X-a_1)(X-a_2) \ldots (X-a_n)}{(X-b_1)(X-b_2) \ldots (X-b_n)} .$$

Replace u by $W = u(X-b_1)\ldots(X-b_n)$. W satisfies $W^2 = (X-a_1)(X-a_2)\ldots(X-a_n)(X-b_1)\ldots(X-b_n)$. We can eliminate repeated roots. If $a_1 = a_2$ for example, let $Y = W/(X-a_1)$. We get

$$Y^2 = (X-a_3)(X-a_4)\ldots(X-b_n) .$$

In this way, we remove all pairs of equal roots. By the transformation $X \mapsto \frac{X-a_3}{a_4-a_3}$, we can rewrite this equation as

$$Y^2 = X(X-1)(X-\lambda_1)\ldots(X-\lambda_s) .$$

We now want to know what s is in terms of the genus of C. We apply the Riemann-Hurwitz formula (Hartshorne [6], p.301) which says that if $f: X \to Y$ is a finite separable

morphism of curves, d = degree of f , V = ramification index and X has tame ramification, then

$$2g(X) - 2 = d(2g(Y) - 2) + V$$

where g(X) = genus of X , g(Y) = genus of Y . In the hyperelliptic case, $Y=\mathbb{P}^1$, $g(\mathbb{P}^1)=0$, d=2 , so we have

$2g(X)-2 = 2(-2) + V$,

i.e., $2g(X) + 2 = V$.

On the other hand, from the form of our equation, we see that $V = s+2$. Therefore,

$$s+2 = 2(g(X)+1)$$

$$s = 2g(X) .$$

By further transformations we can make s odd by taking λ_s to ∞ . Let $\phi = 1/(x-\lambda_s)$ and replace Y by

$$Y' = \frac{\phi^{g+1} Y}{\sqrt{\prod_{j=1}^{s-1} (\lambda_j-\lambda_s)\cdot\lambda_s(\lambda_s-1)}}$$

Then it is easily seen that

$$Y'^2 = \left(\frac{1}{\lambda_s}+\phi\right)\left(\frac{1}{\lambda_s-1}+\phi\right)\left(\frac{1}{\lambda_s-\lambda_1}+\phi\right)\cdots\left(\frac{1}{\lambda_s-\lambda_{s-1}}+\phi\right) .$$

Now let N be the number of solutions of

$$Y^2 = X(X-1)(X-\lambda_1)\cdots(X-\lambda_{2g-1})$$

over k . Let N_1 be the number of solutions of

$$Y^2 = X(X-u)(X-\lambda_1 u)\cdots(X-\lambda_{2g-1}u)$$

where $\left(\frac{u}{g}\right) = -1$. As before, we compare the number of rational points:

$$N_1 = 1 + \sum_{x \in k} \left(1+\left(\frac{x(x-u)(x-\lambda_1 u)\ldots(X-\lambda_{2g-1}u)}{q}\right)\right)$$

$$= 1 + q + \sum_{x \in k} \left(\frac{\frac{x}{u}(\frac{x}{u} - 1)\ldots(\frac{x}{u} - \lambda_{2g-1})}{q}\right)\left(\frac{u^{2g+1}}{q}\right)$$

$$= 1 + q + \phi_q(1)(\tfrac{u}{q})$$

where

$$\phi_q(1) = \sum_{x \in k} \left(\frac{(\frac{x}{u})(\frac{x}{u} - 1)\ldots(\frac{x}{u} - \lambda_{2g-1})}{q}\right)$$

But $\phi_q(1)$ also equals $N-(q+1)$. Therefore,

$$N_1 = 1+q+(\tfrac{u}{q})(N-(q+1)) \quad . \quad \text{If } (\tfrac{u}{q})=-1 \ ,$$

$$N_1 = 2(q+1) - N \ .$$

Now proceed as in the elliptic case. In summary, we have

<u>Proposition 6</u>. If $Y^2 = X(X-1)(X-\lambda_1)\ldots(X-\lambda_{2g-1})$ is the equation of a hyperelliptic curve C of genus g defined over a finite field $k=\mathbb{F}_q$ of characteristic $\neq 2$, and if w is a reciprocal root of the zeta function of C, then we can find a hyperelliptic curve C' with zeta function having a reciprocal root $-w$. C' has equation

$$Y^2 = X(X-u)(X-\lambda_1 u)\ldots(X-\lambda_{2g-1}u)$$

where $u \in k$ is such that $(\frac{u}{q})=-1$ where $(\frac{\cdot}{q})$ denotes the Legendre symbol. C' is a k'/k-form for C where k'

is the quadratic extension of k .

Proof: We first check that C' is a form for C over the quadratic extension k' of k . Let $t=\sqrt{u}$ and consider the morphism $C \to C'$ which sends a point $(x,y) \to (t^2x, t^{2g+1}y)$. We check that this map is well defined:

$$t^{(2g+1)2}\, y^2 = t^2x(t^2x-t^2)(t^2x-t^2\lambda_1)\ldots(t^2x-t^2\lambda_{2g-1})$$

$$= t^{2(2g+1)}\, x(x-1)(x-\lambda_1)\ldots(x-\lambda_{2g-1}) ,$$

so the image of this map satisfies the equation for C' . Since $t^2=u$, $t^{2g+1}=u^g\cdot\sqrt{u}$, this map is defined over k' . It is easy to see this map is an isomorphism. If $\{\alpha_i\}$ is the set of $2g$ roots of the zeta function of C , and $\{\beta_i\}$ the set of $2g$ roots of the zeta function of C' , our previous argument in the elliptic curve case shows that $\Sigma\alpha_i = -\Sigma\beta_i$. On the other hand, C and C' become isomorphic over k' , i.e.,

$$C \otimes_k k' \simeq C' \otimes_k k' .$$

This implies that $\mathrm{Zeta}(C \otimes_k k') = \mathrm{Zeta}(C' \otimes_k k')$, so in particular these have the same roots. But the roots of $\mathrm{Zeta}(C \otimes_k k')$ are $\{\alpha_i^2\}$ and the roots of $\mathrm{Zeta}(C' \otimes_k k')$ are $\{\beta_i^2\}$. Therefore, for each α_i there exists β_j st. $\alpha_i^2 = \beta_j^2$, i.t., $\alpha_i = \pm\beta_j$.

We want to conclude that $\alpha_i = -\beta_j$. To do this, we pass to the Jacobians $J(C)$, $J(C')$ of C and C' respectively. Let Ψ be the k'-isomorphism between $C \otimes_k k'$ and $C' \otimes_k k'$. Ψ passes to a k'-isomorphism

between $J(C) \otimes_k k'$ and $J(C') \otimes_k k'$ which we also call Ψ. Let π be the Frobenius of $J(C)$ and π' the Frobenius of $J(C')$. If $G=gal(k'/k)$, then $G \tilde{=} \mathbb{Z}/2\mathbb{Z} = \{e,\sigma\}$ where e is the identity and σ sends $t=\sqrt{u}$ to $-t$. Let $\tau = \Psi^{-1}\Psi^{\sigma} \in Aut_k(J(C))$. σ has the same effect as π and π' on points of $J(C)$ and $J(C')$ respectively, i.e., σ is the q^{th}-power map. Therefore,

$$\Psi\tau\pi\Psi^{-1} = \Psi\Psi^{-1}\Psi^{\sigma}\ \pi\ \Psi^{-1}$$

$$= \pi'\Psi\ \pi^{-1}\pi\Psi^{-1} = \pi' .$$

That is, the following diagram commutes

$$\begin{array}{ccc} J(C) \otimes k' & \xrightarrow{\Psi} & J(C') \otimes k' \\ \downarrow{\scriptstyle \tau\pi} & & \downarrow{\scriptstyle \pi'} \\ J(C) \otimes k' & \xrightarrow{\Psi} & J(C') \otimes k' \end{array}$$

Since $\tau^2 = 1$, τ is $+1$ or -1. τ is not the identity since Ψ defines a non-trivial form for $J(C)$. The reason we know that τ defines a non-trivial form for $J(C)$ is that Ψ is the image by J of the hyperelliptic involution $(x,y) \mapsto (x,-y)$, hence is -1. We check this directly: If (x,y) is a rational point of C,

$$\Psi^{-1}\Psi^{\sigma}(x,y) = \Psi^{-1}\sigma\ \Psi(x,y)$$

$$= \Psi^{-1}\sigma(t^2x, t^{2g+1}y)$$

$$= \Psi^{-1}(t^2x, -t^{2g+1}y)$$

$$= (x,-y) .$$

Hence, the eigenvalues of $\tau\pi$ and π' are the same on $\underline{H}^1_\ell(J(C)) \simeq \underline{H}^1_\ell(C)$ and $\underline{H}^1_\ell(J(C')) \simeq \underline{H}^1_\ell(C')$ respectively (see Chapter 3 or Milne [13] or SGA 4½ for the definition of ℓ-adic cohomology). But the above shows that the eigenvalues of $\tau\pi$ are -1 times the eigenvalues of π. This proves that $\alpha_i = -\beta_j$ as asserted.

Chapter 2

An Application to Exponential Sums

In this section we use an observation about forms for curves to prove that the roots of the L-function of an Artin-Schreier cover of an algebraic curve defined over a finite field differ from the roots of the zeta function of the cover by roots of unity. This result is in the spirit of the first chapter. This question was raised by Bombieri in [3] and [4].

Let X be an absolutely irreducible normal variety defined over $k = \mathbb{F}_q \equiv [q]$. In this chapter we will use Bombieri's convenient notation so that $[q]$ means the finite field with q elements.

Let $k(X)$, $\bar{k}(X)$ be the function field of X over k and over $\bar{k}$, $\bar{k}$ = an algebraic closure of k. Let $R(X) \in k(X)$ be a rational function on X such that $R(x) \neq h^p - h$ for $h \in \bar{k}(X)$. R defines a map $X \to A^1$ where A^1 is the affine line over $[q]$. Let X_m be the set of points of X defined over $[q^m]$, and

$$S_m(R,X) = \sum_{x \in X_m}{}' \exp\left[\frac{2\pi i}{p} \mathrm{tr}(R(x))\right]$$

where $'$ means exclude the points lying on the poles of $R(x)$ and $\mathrm{tr}: [q] \to [p]$ is the absolute trace.

Let X' be the variety defined by $Z^p - Z = R(x)$. Then there is a Galois covering $\begin{array}{c} X' \\ \downarrow \pi \\ X \end{array}$ $\begin{array}{c} (z,x) \\ \downarrow \\ x \end{array}$. This covering has Galois group $\mathbb{Z}/p\mathbb{Z}$ acting on X' by

$$g: (z,x) \longrightarrow (z+g,x) .$$

It is easily checked that $(z+g,x)\in X'$. Let Y be a normalization of X' , so there exists a birational map $r: Y\to X'$. By composing $\pi\circ r = f$, we get an Artin-Schreier covering of X related to $R(x)$. Define an L-function related to this covering by

$$L(t,R,X) \equiv \exp \sum_{m=1}^{\infty} S_m(R,X)t^m/m .$$

Bombieri [4] calls this the Artin L-function associated with the Artin-Schreier covering $f: Y\to X$.

We now state Bombieri's theorem. Let Y be the Artin-Schreier cover associated to $\mathbf{Z}^p-Z = R(x), x\in X$. Let $Y(\lambda)$ be the Artin-Schreier cover associated to $\mathbf{Z}^p-\mathbf{Z} = R(x) + \lambda$, $\lambda\in[q^p]$.

Theorem 2. (Bombieri [4]). $L(t,R,X)$ is a rational function of t . There exists a suitable power p^μ of the degree p of the cover $\pi: Y\to X$ such that if Θ is a characteristic root of $L(t,R,X)$, then there exists $\nu \leq \mu-1$ and $\lambda\in[q^p]$ such that

$$\Theta^{p^\mu} = W^{p^{\mu-\nu}} .$$

where W is a characteristic root (zero or pole) of $Z(t,Y(\lambda),q^{p^\nu})$, the zeta function of $Y(\lambda)$ relative to the ground field $[q^{p^\nu}]$.

At the end of the papers [ ] and [ ] Bombieri conjectures that Θ is of the form $\Theta = \gamma W_1$ where W_1 is a characteristic root of $Z(T,Y,q)$ and γ is a p^μ-th root of unity. We give a proof of this statement.

In recent communication Bombieri has informed us that the conjecture can also be proved by considering the Frobenius action on ℓ-adic cohomology.

Lemma 2. If W is a characteristic root of $Z(t,Y(\lambda),q^{p^\nu})$, $\lambda \varepsilon \mathrm{Im}(\mathrm{tr}([q^{p^{\nu+1}}]))$, then W^p is a characteristic root of $Z(t,Y,q^{p^{\nu+1}})$.

Proof: Choose $\lambda \varepsilon [q^{p^\nu}]$ so that there exists $\lambda' \varepsilon [q^{p^{\nu+1}}]$ such that $\lambda'^p - \lambda' = \lambda$. Therefore,

$$Z^p - Z = R(x) + \lambda = R(x) + \lambda'^p - \lambda' ,$$

i.e., $$(Z-\lambda')^p - (Z-\lambda') = R(x) .$$

Thus, $Y(\lambda)$ and Y are $[q^{p^{\nu+1}}]/[q^{p^\nu}]$- forms. Therefore the eigenvalues of their Frobenii acting on ℓ-adic cohomology must differ by roots of unity. The argument here is similar to the hyperelliptic curve case in Chapter 1. Since W is a characteristic root of $Z[t,Y(\lambda),q^{p^\nu}]$, ζW is a characteristic root of $Z[t,Y,q^{p^\nu}]$, where ζ is some p^{th} root of unity; i.e., $\zeta^p W^p = W^p$ is a characteristic root of $Z[t,Y,q^{p^{\nu+1}}]$. This proves the lemma.

Now observe that $(W^p)^{p^{-\nu-1}} = W^{p^{-\nu}}$ is a characteristic root of $Z[t^{p^{\nu+1}},Y,q^{p^{\nu+1}}]$, and we have the following fact:

$$Z[t^{p^{\nu+1}},Y,q^{p^{\nu+1}}] = \prod_{\zeta} Z[\zeta t,Y,q]$$

where the product is over all the $p^{\nu+1}$-st roots of unity.

It is easy to see this. Recall that in general, the

zeta function of a smooth variety X defined over $[q]$ has the following form as a rational expression:

$$Z(X,t) = \frac{P_1(t)P_3(t) \ldots P_{2n-1}(t)}{P_o(t)P_1(t) \ldots P_{2n}(t)}$$

where $n=\dim X$, $P_o(t) = 1-t$, $P_{2n}(t)= 1-q^n t$, $P_i(t)= \prod_j (1-\alpha_{ij}t)$. and the $P_i(t)$'s have coefficients in $\mathbb{Z}$. Therefore the zeta function takes the form

$$Z(X,t) = \prod_i \prod_j (1-\alpha_{ij}t)^{(-1)^{i+1}}$$

In our case, a factor on the right hand side, $Z[\zeta t,Y,q]$ has the form

$$Z[\zeta t,Y,q] = \prod_i \prod_j (1-a_{ij}\zeta t)^{(-1)^{i+1}} .$$

$Z[t^{p^{\nu+1}},Y,q^{p^{\nu+1}}]$ has the form

$$Z[t^{p^{\nu+1}},Y,q^{p^{\nu+1}}] = \prod_i \prod_j (1-\beta_{ij}t^{p^{\nu+1}})^{(-1)^{(i+1)}} .$$

The numerators of these zeta functions are characteristic polynomials of Frobenius acting on $\underline{H}^i_\ell(Y)$. When we raise the ground field from $[q]$ to $[q^{p^{\nu+1}}]$, to get the correct Frobenius, we must iterate the q-Frobenius $p^{\nu+1}$ times. The eigenvalues for the iterated Frobenius are those for the q-Frobenius raised to the $p^{\nu+1}$-st power. Thus, we have that

$\beta_{ij} = \alpha_{ij}^{p^{\nu+1}}$. Therefore the zeta function becomes

$$Z[t^{p^{\nu+1}},Y,q^{p^{\nu+1}}] = \prod_j (1-(\alpha_{ij}t)^{p^{\nu+1}})$$

which factors as

$$\prod_\zeta (\prod_i \prod_j (1-\alpha_{ij}\zeta t)^{(-1)^{i+1}})$$

where the product is over all the $p^{\nu+1}$-st roots of unity. But this expression is precisely $\prod_\zeta Z[\zeta t,Y,q]$. By this fact, we must have that $W^{p^{-\nu}}$ is a characteristic root of one of the $Z(\zeta t,Y,q)$'s . Therefore we have proved

Lemma 3: If W is a characteristic root of $Z[t,Y(\lambda),q^{p^\nu}]$, then $W^{p^{-\nu}} = \zeta\xi$ where ξ is a characteristic root of $Z[t,Y,q]$ and ζ is a $p^{\nu+1}$-st root of unity.

By Bombieri's theorem, we have that if Θ is a characteristic root of $L(t,R,X)$, then

$$\Theta^{p^\mu} = W^{p^{\mu-\nu}} = (W^{p^{-\nu}})^{p^\mu} \quad , \ \nu \leq \mu-1$$

and W is a characteristic root of $Z[t,Y(\lambda),q^{p^\nu}]$ for some $\lambda\varepsilon[q^{p^\nu}]$. Taking p^μ-th roots on both sides, we get

$$\Theta = \eta W^{p^{-\nu}} = \eta\zeta\xi = (\eta\zeta)\xi$$

where η is a p^{μ}-th root of unity, ζ is a $p^{\nu+1}$-st root of unity and ξ is a characteristic root of $Z[t,Y,q]$. Since $\nu+1 \leq \mu$, it is easily seen that $\eta\zeta$ is a p^{μ}-th root of unity. Let $\gamma=\eta\zeta$, $W_1=\xi$ we get

Proposition 7: Notation as above. Then $\Theta = \gamma W_1$ where γ is a p^{μ}-th root of unity and W_1 is a characteristic root of $Z[t,Y,q]$.

Chapter 3

On the Norm of an Algebraic Curve

In this chapter we recall the definition and some properties of the Picard functor. In particular, we show that the norm and Picard functors commute up to isomorphism. We use the commutativity of $N_{k'/k}$ and $\underline{Pic}^\circ$ to produce a correspondence between $N_{k'/k}$ of an algebraic curve C over k' and a product $C_o \times \ldots \times C_r$ of twisted forms for C. This is our attempt to generalize the isogeny factorization of the norm.

We first recall basic definitions and facts about the relative Picard functor. References here are Oort [6] and Grothendieck [5]. If X is an S-scheme with structure morphism f, and $T \to S$ is a change of base, $f_T: X_T \to T$ denotes the projection onto T,

$$\begin{array}{ccc} X_T = X \times_S T & \longrightarrow & X \\ \downarrow{\scriptstyle f_T} & & \downarrow{\scriptstyle f} \\ T & \longrightarrow & S \end{array} .$$

Define the relative Picard functor $\underline{Pic}_{X/S}$ to be the sheaf for the flat topology associated to the functor which sends an S-scheme T to $R^1 f_{T_*}(\Theta^*_{X_T})$, the first right-derived functor of the push forward along f_T of the sheaf of units $\Theta^*_{X_T}$.

From here on, we assume that X/S is projective and smooth. $\underline{Pic}^\circ_{X/S}$ denotes the connected component of the identity of $\underline{Pic}_{X/S}$. Under the projective smooth assumption, $\underline{Pic}^\circ_{X/S}$ has the structure of abelian scheme

over S. We shall use several properties of $\underline{\mathrm{Pic}}^{\circ}_{X/S}$. One of these is that $\underline{\mathrm{Pic}}^{\circ}_{X/S}$ commutes with base change, i.e. if $S' \to S$ is a change of base, then $\mathrm{Pic}_{X_{S'}/S'} \tilde{=} \mathrm{Pic}^{\circ}_{X/S} \times_S S'$. Another fact is that if X is an algebraic curve, $\underline{\mathrm{Pic}}^{\circ}_{X/S}$ is the Jacobian of X (see Hartshorne [6]). For further information about representability of $\underline{\mathrm{Pic}}_{X/S}$, see, e.g., Artin [1], Grothendieck [5], Murre [15], Oort [16].

We now need to define correspondences and recall some basic facts about them. Our reference here is Hoobler [8].

Definition: If X is a smooth, proper variety over a field k, the Albanese variety of X is defined by

$$A(X) \equiv \underline{\mathrm{Pic}}^{\circ}_{\underline{\mathrm{Pic}}^{\circ}_{X/k}} .$$

By a k-pointed variety we mean a pair (X, x_o) where X is a smooth, proper variety over k and x_o is a k-rational point of X.

Definition: If (X, x_o), (Y, y_o) are k-pointed varieties, define a divisorial correspondence between X and Y to be a line bundle L over $X \times Y$ such that $L|_{X \times \{y_o\}} \tilde{=} \Theta_X$ and $L|_{\{x_o\} \times Y} \tilde{=} \Theta_Y$, where Θ_X and Θ_Y are the structure sheaves for X and Y respectively.

Definition: If X has structure map $p: X \to \mathrm{Spec}\ k$, the ℓ-adic cohomology sheaf is defined by

$$\underline{H}^i_{\ell}(X) \equiv \varprojlim_n R^i p_* \mu_{\ell^n}^{\otimes i} .$$

Lemma 4: If A is an abelian variety over k, then $\underline{H}^*_{\ell}(A) \tilde{=} \Lambda^* \underline{H}^1_{\ell}(A)$. In particular, $H^2_{\ell}(A)$ is generated by cup product from $\underline{H}^1_{\ell}(A)$.

Proof: Serre [18].

Definition: If X is a variety over k, define the Neron-Severi sheaf

$$NS_{X/k} \equiv (\underline{Pic}_{X/k}) \,/\, (\underline{Pic}^{\circ}_{X/k}) .$$

The Brauer group sheaf $Br'(X)$ is defined by $Br'(X) = R^2p_*(\Theta_X^*)$. If F is any sheaf over X, define $T_\ell F$ by $T_\ell F = \varprojlim_n F/_{\ell^n F}$.

Lemma 5: The following sequence is exact:

$$0 \to \underline{NS}_{x/k} \otimes \hat{\mathbb{Z}}_\ell(1) \to \underline{H}^2_\ell(X) \to T_\ell(\underline{Br}'(X))\ (1) \to 0$$

where ℓ is not equal to the characteristic of k.

Proof: Recall that we have the Kummer sequence

$$0 \longrightarrow \mu_{\ell^n} \longrightarrow \Theta_X^* \xrightarrow{\ell^n} \Theta_X^* \longrightarrow 0 ,$$

Milne [ ]. This gives a long exact sequence part of which is:

$$R^1p_*\mu_{\ell^n} \longrightarrow R^1p_*\Theta_X^* \xrightarrow{\ell^n} R^1p_*\Theta_X^* \longrightarrow$$

$$\longrightarrow R^2p_*\mu_{\ell^n} \longrightarrow R^2p_*\Theta_X^* \xrightarrow{\ell^n} R^2p_*\Theta_X^*$$

$$\longrightarrow \cdots$$

But $R^1p_*\Theta_X^* = \underline{Pic}_{X/k}$ and

$$R^2p_*\mu_{\ell^n} = \underline{H}^2(X,\mu_n^{\otimes 2}) \otimes \mu_{\ell^n}^{-1} .$$

Therefore the sequence becomes

$$0 \longrightarrow (\underline{Pic}_{X/k}) \,/\, (\ell^n \underline{Pic}_{X/k}) \longrightarrow H^2(X,\mu_{\ell^n}^{\otimes 2})\ (-1)$$

$$\longrightarrow {}_{\ell^n}R^2p_*\Theta_X^* \longrightarrow 0$$

where $\underline{H}^2(X,\mu_{\ell^n}^{\otimes 2})(-1) = \underline{H}^2(X,\mu_{\ell^n})$.

Letting n vary, we get a sequence of such diagrams

$$0 \longrightarrow \varprojlim_n (\underline{Pic}_{X/k} / \ell^n \underline{Pic}_{X/k}) \longrightarrow \underline{H}^2_\ell(X)(-1) \longrightarrow T_\ell(\underline{Br}'(X)) \longrightarrow 0 .$$

Since $\underline{Pic}^{\circ}_{X/k}$ is an abelian variety, it is ℓ-divisible (Mumford [14]). Hence,

$$(\underline{Pic}_{X/k}) / (\ell^n \underline{Pic}_{X/k}) \simeq \underline{NS}_{X/k} / \ell^n \underline{NS}_{X/k} .$$

Also, $\varprojlim_n \underline{NS}_{X/k} / \ell^n \underline{NS}_{X/k} \simeq \underline{NS}_{X/k} \otimes \hat{\mathbb{Z}}_\ell$

since $\underline{NS}_{X/k}$ is a free, finitely generated locally constant sheaf of abelian groups (Mumford [14]). Therefore the sequence becomes

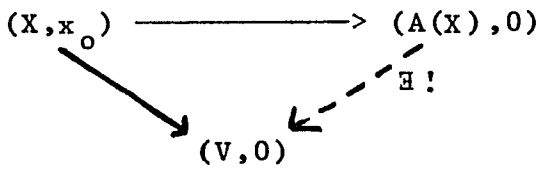
$$0 \longrightarrow \underline{NS}_{X/k} \otimes \hat{\mathbb{Z}}_\ell \longrightarrow \underline{H}^2_\ell(X)(-1) \longrightarrow T_\ell(\underline{Br}'(X)) \longrightarrow 0 .$$

Now twist this sequence to get

$$0 \longrightarrow \underline{NS}_{X/k} \otimes \hat{\mathbb{Z}}_\ell(1) \longrightarrow \underline{H}^2_\ell(X) \longrightarrow T_\ell(\underline{Br}'(X))(1) \longrightarrow 0$$

which proves the lemma.

Now recall that the Albanese A(X) has the following universal property:



maps from (X,x_o) to abelian varieties $(V,0)$ factor uniquely through $(A(X),0)$.

Lemma 6: Let $\alpha: (X,x_o) \to (A(X),0)$ be the universal map for the Albanese variety, where X is projective and smooth over k. Then α induces an isomorphism $\underline{H}^1_\ell(A(X)) \simeq \underline{H}^1_\ell(X)$.

Proof: By duality, $\hat{\alpha}$ induces a map

$$\hat{\alpha}: \underline{Pic}^\circ_{A(X)/k} \longrightarrow \underline{Pic}^\circ_{X/k} .$$

But $\underline{Pic}^\circ_{A(X)/k} \simeq \underline{Pic}^\circ_{X/k}$, so $\hat{\alpha}$ is an isomorphism. From the Kummer sequence we get the sequence

$$0 \longrightarrow R^1p_*\mu_{\ell^n} \longrightarrow R^1p_*\Theta_X^* \xrightarrow{\ell^n} R^1p_*\Theta_X^*$$

which implies that ${}_{\ell^n}\underline{Pic}^\circ_{X/k} \simeq R^1p_*\mu_{\ell^n}$. Passing to $\varprojlim_n$ gives $T_\ell(\underline{Pic}^\circ_{X/k}) \simeq \underline{H}^1_\ell(X)$. Since $\hat{\alpha}$ is an isomorphism, we also have $T_\ell(\underline{Pic}^\circ_{A(X)/k}) \simeq H^1_\ell(A(X))$ and $T_\ell(\underline{Pic}^\circ_{A(X)/k}) \simeq T_\ell(\underline{Pic}^\circ_{X/k}) \simeq \underline{H}^1_\ell(X)$. Therefore, $\underline{H}^1_\ell(A(X)) \simeq \underline{H}^1_\ell(X)$.

We finally arrive at the theorem about correspondences that we need. Let $Corr(X,Y)$ denote the divisorial correspondences between X and Y.

Theorem 3: Let $(X,x_o),(Y,y_o)$ be k-pointed projective, smooth varieties with $k=\mathbb{F}_q$, the finite field with q elements. Then

$$Corr(A(X),A(Y)) \otimes \hat{\mathbb{Z}}_\ell \simeq Corr(X,Y) \otimes \hat{\mathbb{Z}}_\ell ,$$

where ℓ is a prime not equal to the characteristic of $\mathbb{F}_q$.

Proof: $Corr(X,Y)$ is by definition the kernel of the map $Pic(X\times Y) \to P(X\times y_o) \times Pic(x_o\times Y)$ which sends a line bundle L over $X\times Y$ to $(L|_{X\times y_o}, L|_{x_o\times Y})$. That is, we have

$$\mathrm{Corr}(X,Y) \longrightarrow \mathrm{Pic}(X\times Y) \longrightarrow \mathrm{Pic}(X\times y_o) \times \mathrm{Pic}(x_o\times Y) .$$

There is a section $\mathrm{Pic}(X\times y_o) \times \mathrm{Pic}(x_o\times Y) \to \mathrm{Pic}(X\times Y)$ which sends (L_1,L_2) to $p_1^*L_1 \otimes p_2^*L_2$ where p_1,p_2 are the projective maps. Therefore, $\mathrm{Corr}(X,Y)$ is a summand of $\mathrm{Pic}(X\times Y)$. Passing to the algebraic closure, $\underline{H}^2_\ell(X\times Y)$ decomposes as

$$\underline{H}^2_\ell(\overline{X\times Y}) \simeq \underline{H}^2_\ell(\bar{X}) \oplus \underline{H}^2_\ell(\bar{Y}) \oplus (\underline{H}^1_\ell(\bar{X}) \otimes \underline{H}^1_\ell(\bar{Y}))$$

using the Kunneth formula ($\bar{X}$ means $X \otimes_k \bar{k}$).

By the argument in Lemma 5,

$$[\mathrm{Pic}(\bar{X}\times y_o) \oplus \mathrm{Pic}(x_o\times\bar{Y})] \otimes \hat{\mathbf{Z}}_\ell$$

injects into $\underline{H}^2_\ell(\bar{X}) \oplus \underline{H}^2_\ell(\bar{X})$. Hence $\mathrm{Corr}(\bar{X},\bar{Y}) \otimes \hat{\mathbf{Z}}_\ell$ injects into $\underline{H}^1_\ell(\bar{X}) \otimes \underline{H}^1_\ell(\bar{Y})$. By "Galois theory" (Milne [13], pg.53), we conclude that $\mathrm{Corr}(X,Y) \otimes \hat{\mathbf{Z}}_\ell$ injects into $\underline{H}^1_\ell(X) \otimes \underline{H}^1_\ell(Y)$.

On the other hand, there is a commutative diagram

$$\begin{array}{ccc} \mathrm{Corr}(A(X),A(Y)) \otimes \hat{\mathbf{Z}}_\ell & \hookrightarrow & \underline{H}^1_\ell(A(X)) \otimes \underline{H}^1_\ell(A(Y)) \\ \downarrow & & \downarrow \\ \mathrm{Corr}(X,Y) \otimes \hat{\mathbf{Z}}_\ell & \hookrightarrow & \underline{H}^1_\ell(X) \otimes \underline{H}^1(Y) \end{array}$$

where the dotted arrow is the map induced by pulling back line bundles along

$$X\times Y \longrightarrow A(X) \times A(Y) .$$

But then the dotted arrow is an injection since the other

three arrows are. Hence,

$$\mathrm{Corr}(A(X),A(Y)) \otimes \hat{Z}_\ell \longrightarrow \mathrm{Corr}(X,Y) \otimes \hat{Z}_\ell$$

is an injection. On the other hand, by the fact that the Brauer group of an abelian variety over a finite field is finite.

$$\mathrm{Corr}(A(X),A(Y)) \otimes \hat{Z}_\ell \simeq \underline{H}^1(A(X)) \otimes \underline{H}^1_\ell(A(Y)) .$$

Thus $\mathrm{Corr}(X,Y) \otimes \hat{Z}_\ell$ injects into $\mathrm{Corr}(A(X)),A(Y)) \otimes \hat{Z}_\ell$. This proves the theorem.

In the proof of Lemma 6, we saw that $T_\ell(\underline{\mathrm{Pic}}^\circ_{X/k}) \simeq H^1_\ell(X)$. Therefore, for a product $X \times Y$ we get

$$T_\ell(\underline{\mathrm{Pic}}^\circ_{X\times Y/k}) \simeq \underline{H}^1_\ell(X\times Y) \simeq \underline{H}^1_\ell(X) \oplus \underline{H}^1_\ell(Y)$$

$$\simeq T_\ell(\underline{\mathrm{Pic}}^\circ_{X/k}) \oplus T_\ell(\underline{\mathrm{Pic}}^\circ_{Y/k})$$

by the Kunneth formula. This suggests that $\underline{\mathrm{Pic}}^\circ_{X\times Y/k}$ preserves products, i.e.,

$$f: \underline{\mathrm{Pic}}^\circ_{X\times Y/k} \simeq \underline{\mathrm{Pic}}^\circ_{X/k} \times \underline{\mathrm{Pic}}^\circ_{Y/k} .$$

Consider the map $\mathrm{Pic}(X\times Y) \to \mathrm{Pic}(X) \times \mathrm{Pic}(Y)$ which sends a line bundle L over $X\times Y$ to $L|_{X\times y_o} \times L|_{x_o\times Y}$ where x_o, y_o are base points for X and Y respectively. Note that $\mathrm{Corr}(X,Y)$ is precisely the kernel of this map. This map induces a map

$$\underline{\mathrm{Pic}}^\circ_{X\times Y/k} \longrightarrow \underline{\mathrm{Pic}}^\circ_{X/k} \times \underline{\mathrm{Pic}}^\circ_{Y/k}$$

which is surjective because the base points give a section. We want to show injectivity, i.e., we want to show that

$\mathrm{Corr}(X,Y) \cap \underline{\mathrm{Pic}}^{\circ}_{(X\times Y)/k} = 0$. But $\mathrm{Corr}(X,Y) \otimes \hat{\mathbf{Z}}_\ell$ injects into $\underline{H}^2_\ell(X\times Y)$. Also $\underline{\mathrm{NS}}_{(X\times Y)/k} \otimes \hat{\mathbf{Z}}_\ell$ injects into $H^2_\ell(X\times Y)$. Therefore, $\underline{\mathrm{Pic}}^{\circ}_{(X\times Y)/k} \otimes \hat{\mathbf{Z}}_\ell$ gets sent to 0 in $\underline{H}^2_\ell(X\times Y)$.

It may be possible that there is common ℓ-torsion, but since ℓ is any prime $\neq \mathrm{char}(k)$, this cannot happen.

This leaves the possibility of common p-torsion where $p = \mathrm{char}(k)$. Since the above map f is surjective, we have an exact sequence

$$0 \longrightarrow \ker(f) \longrightarrow \underline{\mathrm{Pic}}^{\circ}_{X\times Y/k} \longrightarrow \underline{\mathrm{Pic}}^{\circ}_{X/k} \times \underline{\mathrm{Pic}}^{\circ}_{Y/k} \longrightarrow 0 .$$

As previously noted,

$$T_\ell(\underline{\mathrm{Pic}}^{\circ}_{X\times Y/k}) \simeq \underline{H}^1_\ell(X) \oplus \underline{H}^1_\ell(Y)$$

$$\simeq T_\ell(\underline{\mathrm{Pic}}^{\circ}_{X/k}) \oplus T_\ell(\underline{\mathrm{Pic}}^{\circ}_{Y/k}) .$$

Therefore, $\dim(\underline{\mathrm{Pic}}^{\circ}_{X\times Y/k}) = \dim(\underline{\mathrm{Pic}}^{\circ}_{X/k} \times \underline{\mathrm{Pic}}^{\circ}_{Y/k})$, so $\ker(f)$ is finite. Since the exact sequence has a section, $\underline{\mathrm{Pic}}^{\circ}_{X\times Y/k} \simeq \underline{\mathrm{Pic}}^{\circ}_{X/k} \oplus \underline{\mathrm{Pic}}^{\circ}_{Y/k} \oplus \ker(f)$. Now the assertion follows since $\underline{\mathrm{Pic}}^{\circ}_{X\times Y/k}$ is connected and reduced by definition.

Now let Y be a smooth proper k'-variety and X a k-variety. By the defining adjointness property of the norm functor, we have the following bijection of sets:

$$\begin{aligned} &\mathrm{Hom}_k(\underline{\mathrm{Pic}}^\circ(N_{k'/k}Y)/k \ , \ N_{k'/k}(\underline{\mathrm{Pic}}^\circ Y/k')) \simeq \\ &\mathrm{Hom}_{k'}(\underline{\mathrm{Pic}}^\circ(N_{k'/k}Y)_{k'}/k' \ , \ \underline{\mathrm{Pic}}^\circ Y/k') \end{aligned} \tag{1}$$

Recall (Chapter 1, Proposition 1) that over k', $N_{k'/k}Y \otimes k' \simeq \prod_{\sigma\in G} Y^\sigma$ where $G = \mathrm{Gal}(k'/k)$. Hence,

$$\underline{\mathrm{Pic}}^\circ(N_{k'/k}Y)_{k'}/k' \simeq \underline{\mathrm{Pic}}^\circ(\prod_{\sigma\in G} Y^\sigma)/k' . \tag{2}$$

Since $\underline{\mathrm{Pic}}^\circ$ preserves products, the right hand side is isomorphic to

$$\prod_{\sigma\in G} \underline{\mathrm{Pic}}^\circ Y^\sigma/k' . \tag{3}$$

Since $\underline{\mathrm{Pic}}^\circ$ commutes with base change,

$$\prod_{\sigma\in G} \underline{\mathrm{Pic}}^\circ Y^\sigma/k' \simeq \prod_{\sigma\in G} \underline{\mathrm{Pic}}^{\circ\sigma} Y/k' \simeq N_{k'/k}(\underline{\mathrm{Pic}}^\circ Y/k') \tag{4}$$

By projection onto the first factor, we have a map

$$\prod_{\sigma\in G} \underline{\mathrm{Pic}}^{\circ\sigma} Y/k' \longrightarrow \underline{\mathrm{Pic}}^\circ Y/k' . \tag{5}$$

Therefore, by composing (2),(3),(4),(5), we get a map

$$\underline{\mathrm{Pic}}^\circ(N_{k'/k}Y)_{k'}/k' \longrightarrow \underline{\mathrm{Pic}}^\circ Y/k' . \tag{6}$$

defined over k' . The adjointness bijection (1) gives a corresponding map

$$f: \underline{\mathrm{Pic}}^{\circ}(N_{k'/k}Y) \longrightarrow N_{k'/k}\,\underline{\mathrm{Pic}}^{\circ}Y/k' \qquad (7)$$

defined over k . We wish to show that f is an isomorphism. The idea of the proof is as follows: tensor f with k' and show that $f \otimes k'$ is an isomorphism. Then, by descent theory, f must be an isomorphism.

Tensoring with k' gives a map

$$f \otimes k': \underline{\mathrm{Pic}}^{\circ}(N_{k'/k}Y)_{k'}/k' \longrightarrow (N_{k'/k}\,\underline{\mathrm{Pic}}^{\circ}Y/k') \otimes k' \qquad (8) .$$

Let T be a k'-variety regarded as a "test object". Consider the following diagram

$$\begin{array}{ccc} \mathrm{Hom}_{k'}(T, \underline{\mathrm{Pic}}^{\circ}(N_{k'/k}Y)_{k'}/k') & \xrightarrow[g]{\simeq} & \mathrm{Hom}(T, \prod_{\sigma} \underline{\mathrm{Pic}}^{\circ\sigma}Y/k') \\ \Big\downarrow f \otimes k' & \nearrow_{h}^{\simeq} & \\ \mathrm{Hom}_{k'}(T, (N_{k'/k}\,\underline{\mathrm{Pic}}^{\circ}Y/k') \otimes k') & & \end{array} \qquad (9)$$

The dotted arrow is induced by composition with $f \otimes k'$ and the solid arrows are isomorphisms. g is induced by the isomorphisms (2) and (3), and h is induced by the isomorphism coming from the defining property of norm (see Chapter 1). Since g and h are isomorphisms, if we can show that the diagram (9) commutes, we will have that $f \otimes k'$ is an isomorphism.

g sends a map

$$t: T \longrightarrow \underline{\mathrm{Pic}}^{\circ}(N_{k'/k}{}^{Y})_{k'/k} \tag{10}$$

$$\downarrow$$

$$T \xrightarrow{t} \underline{\mathrm{Pic}}^{\circ}(N_{k'/k}{}^{Y})_{k'/k'} \longrightarrow \underline{\mathrm{Pic}}^{\circ}_{\prod_{\sigma} Y^{\sigma}/k'} \longrightarrow \prod_{\sigma} \underline{\mathrm{Pic}}^{\circ}_{Y^{\sigma}/k'} \longrightarrow \prod_{\sigma} \underline{\mathrm{Pic}}^{\circ\sigma}_{Y/k}$$

Going around the other way, we get

$$T \xrightarrow{t} \underline{\mathrm{Pic}}^{\circ}(N_{k'/k}{}^{Y})_{k'/k'} \xrightarrow{f \otimes k'} (N_{k'/k}\underline{\mathrm{Pic}}^{\circ}{}_{Y/k'}) \longrightarrow \prod_{\sigma} \underline{\mathrm{Pic}}^{\circ\sigma}_{Y/k'} \tag{11}$$

We want to show that these maps are equal.

By the adjointness property of the norm, there is a universal map

$$(N_{k'/k}\ \underline{\mathrm{Pic}}^{\circ}{}_{Y/k'}) \otimes k' \longrightarrow \underline{\mathrm{Pic}}^{\circ}{}_{Y/k'} \tag{12}$$

such that the bijection

$$\mathrm{Hom}'_{k'}(\underline{\mathrm{Pic}}^{\circ}(N_{k'/k}{}^{Y})_{k'/k'},\ (N_{k'/k}\ \underline{\mathrm{Pic}}^{\circ}{}_{Y/k'}) \otimes k')$$

$$\simeq \mathrm{Hom}_{k'}(\underline{\mathrm{Pic}}^{\circ}(N_{k'/k}{}^{Y})_{k'/k'}, \underline{\mathrm{Pic}}^{\circ}{}_{Y/k'}) \tag{13}$$

is obtained by composition with (12). The accent on $\mathrm{Hom}_{k'}$ means k'-maps which descend to k-maps; i.e., k'-maps preserving descent data. Therefore the problem reduces to showing that (12) factors through

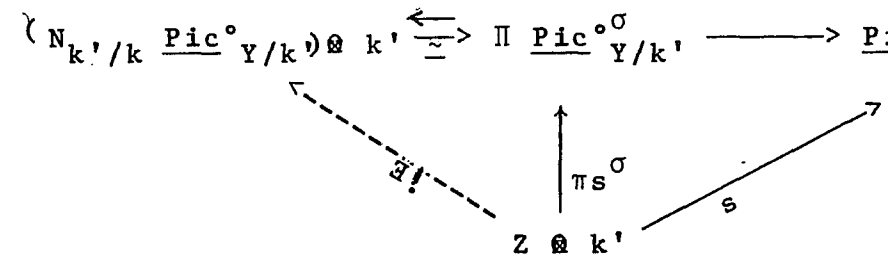
$$(N_{k'/k}\underline{\mathrm{Pic}}^{\circ}{}_{Y/k'}) \otimes k' \xrightarrow{\simeq} \prod_{\sigma} \underline{\mathrm{Pic}}^{\circ\sigma}_{Y/k'} \tag{14}$$

To do this, it suffices to show that

$$(N_{k'/k}\ \underline{\mathrm{Pic}}^{\circ}{}_{Y/k'}) \otimes k' \longrightarrow \prod_{\sigma} \underline{\mathrm{Pic}}^{\circ\sigma}{}_{Y/k'} \longrightarrow \underline{\mathrm{Pic}}^{\circ}{}_{Y/k'} \tag{15}$$

satisfies the appropriate universal property. Therefore, let Z be a k-variety and $s: Z \otimes k' \to \underline{\mathrm{Pic}}^{\circ}{}_{Y/k'}$ a k'-morphism.

s induces a map $\pi s^{\sigma}: Z \otimes k' \to \underline{\mathrm{Pic}}^{\circ\sigma}{}_{Y/k'}$ by pulling back and taking the product. So we get a diagram



The dotted arrow is the composite of πs^{σ} with the inverse to (14). It is the unique arrow which makes the diagram commute. Thus we see that (10) and (11) are equal. We sum this up in

Theorem 4: Norm and $\underline{\mathrm{Pic}}^{\circ}$ commute up to isomorphism if k'/k is Galois; i.e., if Y is a k'-variety,

$$N_{k'/k}\ \underline{\mathrm{Pic}}^{\circ}{}_{Y/k'} \cong \underline{\mathrm{Pic}}^{\circ}{}_{(N_{k'/k}Y)/k}\ .$$

We now recall a proposition from Milne [12]. Let M and M' be R-free G-modules where R is a commutative subring of $\mathrm{End}(A)$ where A is an abelian variety over k, and k'/k is a Galois extension with group G. We assume that M and M' have the same R-rank and that we have isomorphisms

$$\eta: R^n \to M$$

$$\eta': R^n \to M'\ .$$

Lemma 7: If $\phi: M \to M'$ has non-zero determinant $\det(\phi)$ with respect to the R-bases provided by η, η', then ϕ_A (see Chapter 1) is an isogeny of degree $|N_{R/\mathbb{Z}}\det(\phi)|^{2d/r}$ where $d = \dim(A)$ and $r = \operatorname{rank}_{\mathbb{Z}}(R)$.

Proof: Let $F = R \otimes_{\mathbb{Z}} Q$. We may assume that $k = \bar{k}$ (algebraic closure). Then $M_n(F)$ is a simple Q-algebra. Therefore by Mumford [14], pg. 179, it suffices to check that $\deg\phi_A = |N_{F/Q}\det\phi|^{2d/r}$ for $\phi \in \mathbb{Z}$. If $\phi \in \mathbb{Z}$, $\det(\phi) = \phi^n$, and $(N_{F/Q}(\phi^n)^{2d/r} = (\phi^{nr})^{2d/r} = \phi^{2dn}$. This agrees with $\deg\phi_A$ since ϕ_A is a map between forms of dimension dn.

Lemma 8: (Milne [12]). Let A be a k-elementary abelian variety such that $R = \operatorname{End}(A)$ is commutative and all endomorphisms are defined over k. Let $G = \mathrm{Gal}(k'/k)$ and $s: G \to \mathrm{Aut}(A)$ a homomorphism. Then $s(G)$ is cyclic. Let m be the order of $s(G)$. Let R_i, $0 \le i \le m-1$ be R regarded as a G-module by $g \cdot r = s(g)^i \cdot r$ and let $A_i = R_i \otimes_R A$. Let L be the fixed field of $H = \ker s$. Then there is an isogeny of degree M^{md}

$$N_{L/k}(A \otimes_k L) \longrightarrow A_o \times A_1 \times \ldots \times A_{m-1}.$$

Proof: Let σ generate G/H and let $\xi = s(\sigma)$. Consider the homomorphism $\phi: R[G/H] \to \pi R_i$ defined by the matrix (ξ^{ij}) $0 \le i,j \le m-1$. Check that this matrix has determinant $\sqrt{m}^m$ and apply the previous lemma with $r=1$.

To continue, we now reproduce some needed results from Sekiguchi [17].

Theorem 5:Let S' be a faithfully flat S-scheme, C' a non-hyperelliptic curve over S' (i.e. C' has non-hyperelliptic curves as geometric fibers), and P a principally polarized abelian scheme over S having an S'-isomorphism

$$\phi' : J(C') \xrightarrow{\sim} P \otimes_S S' .$$

Then there exist a curve C over S and isomorphisms

$$f' : C \otimes_S S' \xrightarrow{\sim} C'$$

$$\phi : J(C) \xrightarrow{\sim} P$$

such that

$$\phi_{S'} \circ J(f') = \phi' .$$

Here, $J(X)$ means the Jacobian of the algebraic curve X.

The proof of this theorem is based on another theorem of Sekuguchi appearing in the same paper.

Theorem 6:Let C and C' be non-hyperelliptic curves. Let G be the constant group scheme $\{\pm 1\}$. G acts on $\mathrm{Isom}_S(J(C'),J(C))$, the polarization preserving S-isomorphisms between $J(C')$ and $J(C)$, and the geometric quotient $\mathrm{Isom}_S(J(C'),(J(C))/G$ exists. Then, the natural map

$$J : \mathrm{Isom}_S(C,C') \longrightarrow \mathrm{Isom}_S(J(C),J(C'))/G$$

is an isomorphism.

The idea of the proof of Theorem 5, given Theorem 6, is to observe that C' descends, hence carries descent

data, hence descends to a curve C over S. Therefore, $J(C')$ descends to $J(C)$ and to P. So by uniqueness of descent, $J(C) \tilde{-} P$. Sekiguchi also treats the hyperelliptic case. See [17].

Now let X be an algebraic curve smooth and proper over $k=\mathbb{F}_q$. Let $X' = X \otimes_k k'$. Let $Z = \underline{Pic}^\circ_{X'/k'}$ (the Jacobian of X'). Assume that $\underline{Pic}^\circ_{X/k}$ is k-simple and that there is an injective homomorphism

$$Gal(k'/k) \longrightarrow Aut(\underline{Pic}^\circ_{X/k}) .$$

Then by Milne's lemma, there is an isogeny $N_{k'/k}Z \longrightarrow Z_o \times \ldots \times Z_{m-1}$ where m is the degree of the extension k'/k and each Z_i is a k'/k-form for Z. By Sekiguchi's theorem, each Z_i is isomorphic to $\underline{Pic}^\circ_{X_i/k}$ for some algebraic curve X_i over k. Therefore, using properties of $\underline{Pic}^\circ$, we get

$$\begin{aligned} Z_o \times \ldots \times Z_{m-1} &\tilde{=} \underline{Pic}^\circ_{X_o/k} \times \ldots \times \underline{Pic}^\circ_{X_{m-1}/k} \\ &\tilde{-} \underline{Pic}^\circ_{(X_o \times \ldots \times X_{m-1})/k} . \end{aligned}$$

By Theorem 4,

$$N_{k'/k}(\underline{Pic}^\circ_{X'/k'}) \tilde{=} \underline{Pic}^\circ_{(N_{k'/k}X')/k} .$$

Therefore, we get a correspondence

$$\underline{Pic}^\circ_{(N_{k'/k}X')/k} \longrightarrow \underline{Pic}^\circ_{(X_o \times \ldots \times X_{m-1})/k} .$$

Hence by Theorem 3, we get a correspondence

$$N_{k'/k}X' \longrightarrow X_o \times \ldots \times X_{m-1} .$$

As mentioned previously, this result can be viewed as an attempt to generalize the isogeny factorization of the norm by the product of k'/k-forms as in Chapter 1.

This argument makes the assumption that $\underline{Pic}^{\circ}_{X/k}$ is k-simple, which is unnecessarily restrictive. This assumption is made in order to apply Milne's lemma. However, a careful examination of Milne's argument shows that k-simplicity is assumed to ensure that the image of the Galois group G of k'/k in $Aut(A)$ by a map s is cyclic. But Milne is dealing with fields k' and k which are not necessarily finite. Since we are dealing with finite fields k'/k, $s(G)$ is cyclic by necessity. Hence we may lift the assumption of k-simplicity of $\underline{Pic}^{\circ}_{X/k}$.

With regard to the assumption of injectivity of $G = Gal(k'/k) \to Aut(\underline{Pic}^{\circ}_{X/k})$, if we drop this assumption, and if H is the kernel, we can say the following.

If L is the fixed field of H, then $k \subseteq L \subseteq k'$. Milne's lemma gives us an isogeny

$$N_{L/k}\, \underline{Pic}^{\circ}_{X_L/L} \longrightarrow Z_0 \times \ldots \times Z_{m-1}$$

where m is the cardinality of the image $s(G) \subseteq Aut(\underline{Pic}^{\circ}_{X/k})$. Pushing through the above argument gives a correspondence

$$N_{L/k}(X \otimes_k L) \longrightarrow X_0 \times \ldots \times X_{m-1}$$

where each X_i is an L/k-form for X.

We feel that there are further questions of interest in this area. For example, in trying to define two curves X,Y as isogenous if $J(X)$ is isogenous to $J(Y)$, the question arises of whether an abelian variety that is isogenous to a Jacobian is isomorphic to one. Also, is it possible to characterize Weil numbers of Jacobians?

BIBLIOGRAPHY

[1] Artin, M. Théorèmes de représentabilité pour les espaces algébriques, University of Montreal Press, 1971.

[2] Baldisserri, N. Sul numero dei punti di cubiche ellittiche, a moltiplicazione complessa, ridotte modulo p, Bollettino U.M.I., 16-A (1979), pp.367-373.

[3] Bombieri, E. On galois coverings over finite fields, Actas del Coloquio Internacional sobre Geometria Algebraica, Madrid (1965), pp. 23-30.

[4] Bombieri, E. On exponential sums in finite fields, Am. J. Math. 88(1966), pp. 71-105.

[5] Grothendieck, A. Fondements de la Géométrie Algébrique, Sém. Bourbaki 1957-62, Secrétariat Math., Paris (1962).

[6] Hartshorne, R. Algebraic Geometry, Springer-Verlag, (1977).

[7] Honda, T. Isogeny classes of abelian varieties over finite fields, J. Math. Soc. Japan 20(1968), pp.83-95.

[8] Hoobler, R. Personal communication.

[9] Katz, N. An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields, Proc. of Symp. in Pure Math., Vol. XXVII, Amer. Math. Soc. (1976).

[10] Lang, S. Abelian Varieties, Interscience (1959).

[11] Lang, S. Complex Multiplication, Springer-Verlag, (1983).

[12] Milne, J. On the arithmetic of abelian varieties, Invent. Math. 17(1972), pp. 177-190.

[13] Milne, J. Étale Cohomology, Princeton University Press, 1980.

[14] Mumford, D. Abelian Varieties, Oxford University Press, (1970).

[15] Murre, J.P. On contravariant functors from the category of preschemes over a field into the category of abelian groups, Publ. Math. I.H.E.S. No.23, Paris (1964).

BIBLIOGRAPHY (continued)

[16] Oort, F. Sur le schéma de Picard, Bull. Soc. Math., France, 90(1962), pp. 1-14.

[17] Sekiguchi, T. On the fields of rationality for curves and their Jacobian varieties, Nagoya Math. J., 88 (1982), pp. 197-212.

[18] Serre, J.P. Quelques propriétés variétés abéliennes en caracteristique p , Amer. J. Math. 80(1958), pp. 715-739.

[19] Serre, J.P. Local Fields, Springer-Verlag (1979).

[20] Shimura, G. and Taniyama, Y. Complex Multiplication of Abelian Varieties and its Applications to Number Theory, Tokyo (1961).

[21] Springer, G. Introduction to Riemann Surfaces, Addison Wesley (1957).

[22] Tate, J. Endomorphisms of abelian varieties over finite fields, Invent. Math. 2(1966), pp. 134-144.

[23] Tate, J. Classes d'isogenie des variétés abéliennes sur un corps fini (d'après T. Honda), Sém. Bourbaki 1968/69 exposé 352, Springer-Verlag, 1971.

[24] Waterhouse, W. Introduction to Affine Group Schemes, Springer-Verlag (1979).

[25] Waterhouse W. and Milne, J. Abelian varieties over finite fields, Proc. of Symp. in Pure Math. Vol. XX, Amer. Math. Soc. (1971).

[26] Weil, A. Variétés Abéliennes et Courbes Algébriques, Hermann, Paris (1971).

[27] Weil, A. "The field of definition of a variety," Am. J. Math. 78 No.3(1956), pp. 509-524.

[28] Weil, A. Adeles and Algebraic Groups, Institute for Advanced Study (1961).